WHAT IS CLAIMED IS:

1. In an authentication system in which an authentication server which authenticates a user, a user terminal which transmits a user authentication information, and an application server which provides a service to the user through the user terminal are connected together to enable a communication therebetween through a network; an address based authentication system in which

the authentication server comprises

authentication means for authenticating a user based on the user authentication information transmitted as an authentication request from the user terminal;

an address allocating means for allocating an address to the user terminal for a successful authentication of the user;

a ticket issuing means for issuing a ticket containing the address allocated by the address allocating means;

and a ticket transmitting means for transmitting the ticket issued by the ticket issuing means to the user terminal;

the user terminal comprises

a user authentication information transmitting means for transmitting a user authentication information to the authentication server for purpose of an authentication request;

a ticket reception means for receiving a ticket transmitted from the authentication server;

means for setting up an address contained in the ticket as a source address for a packet which is to be transmitted from the user terminal;

means for transmitting a packet including the ticket to the application server for establishing a session;

and a service request means for transmitting a packet requesting a service to the application server;

and the application server comprises

a ticket memory means for storing the ticket transmitted from the user terminal;

an address comparison means for determining whether or not the address contained in the ticket which is stored in the ticket memory means coincides with the source address of the service request packet which is transmitted from the user terminal through the session;

and a service providing means for transmitting to the user a packet which provides a service to the user when a coincidence between the addresses is determined by the address comparison means.

2. An authentication system according to Claim 1

in which the user terminal has a key information relating to a private key of the user terminal,

the user authentication information transmitting means being means for transmitting the key information also together with the user authentication information, and the ticket issuing means being means for issuing a ticket also containing the key information which is transmitted from the user terminal,

the user terminal further comprising

a session key generating means for calculating a session secret key which is shared with the application server from a private key of the user terminal and a public key of the application server;

and a packet cryptographic processing means for performing a processing upon a packet transmitted from the user terminal to guarantee that there is no forgery in the packet by the session secret key;

the application server further comprising

a session key generating means for calculating a session secret key which is shared with the user terminal from the private key of the application server and a public key of the user terminal;

a packet verifying means for confirming whether or not the packet received from the user terminal is forged using the session secret key;

and a ticket verifying means for verifying whether or not the key information contained in the ticket of the packet which has been verified as not being forged is information relating to the private key of the user terminal, the ticket verifying means preventing the ticket from being stored in the ticket memory means when the key information is not a relating information.

3. An authentication system according to Claim 2

in which a transmission of the ticket from the user terminal takes place in terms of a packet,

the application server further comprising

an address collating means for collating the address in the ticket transmitted from the user terminal against the source address of the packet which includes the ticket and for preventing the ticket from being stored if a coincidence is not found.

4. An authentication system according to Claim 2 in which the authentication server comprises a user identifier allocating means for allocating a user identifier which corresponds to the authenticated user in response to the authentication request for a successful authentication of the user,

the ticket issuing means being means for issuing the ticket inclusive of the user identifier.

5. An authentication system according to one of Claims 1 to 4

in which the ticket issuing means of the authentication server

comprises means including an authentication information generating means for generating an authentication information for a provisional ticket using a shared secret key which is shared beforehand between the authentication server and the application server and for issuing the ticket containing the authentication information,

the ticket verifying means of the application server comprising an authentication information verifier for verifying the presence or absence of any forgery in the authentication information contained in the ticket using a shared secret key which is beforehand shared between the authentication server and the application server and for preventing the ticket from being stored in the ticket memory means in the presence of a forgery.

6. An authentication system according to Claim 1 or 4

in which the transmission of the ticket from the user terminal takes place in terms of a packet,

the application server comprising an address collating means for collating the address in the ticket which is transmitted from the user terminal against the source address of the packet which includes the ticket and for preventing the ticket from being stored when a coincidence is not found.

7. An authentication server in an authentication system in which an authentication of a user utilizing a user terminal is performed through the user terminal by an authentication server and a request is made to an application server to provide a service on the basis of the authentication; comprising

a user authentication information reception means for receiving an authentication request inclusive of a user authentication information transmitted from the user terminal;

an authentication means to which the user authentication

information of the received authentication request is input and which authenticates the user on the basis of the user authentication information and providing a signal indicating a successful authentication upon a successful authentication;

an address allocating means for allocating an address to the user terminal in response to an input of the signal indicating a successful authentication of the user;

a ticket issuing means to which the allocated address is input and which issues a ticket containing the address;

and a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal.

8. An authentication server according to Claim 7, further comprising

an authentication information generating means for generating an authentication information for information which includes at least the allocated address using a shared secret key which is beforehand shared between the authentication server and the application server

the ticket issuing means being means for issuing the ticket inclusive of the authentication information.

9. An authentication server according to Claim 7, further comprising

a user identifier allocating means for allocating a user identifier which corresponds to the authenticated user in response to the authentication request when the signal indicating a successful authentication of the user is input,

the ticket issuing means being means for issuing the ticket inclusive of the user identifier.

10. An authentication server according to Claim 9 in which the user identifier allocating means is means to which information which directly identifies the user is input and which encrypts information which directly identifies the user by using an identifier generating secret key of the authentication server, the encrypted information being the user identifier.

11. An authentication server according to one of Claims 7 to 10 in which key information relating to a private key of the user terminal is contained in the authentication request and the ticket issuing means being means for issuing the ticket inclusive of the key information.

12. A user terminal in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication, comprising

a user authentication information transmitting means for transmitting a user authentication information which is input to an authentication server for purpose of an authentication request;

a ticket reception means for receiving a ticket transmitted from the authentication server;

a source address set-up means to which the received ticket is input and which sets up an address contained in the ticket as a source address of the user terminal;

a session establishing means to which the ticket is input and which transmits a packet including the ticket to an application server for establishing a session with the application server;

and a service request means for transmitting a packet representing a service request to the application server through the established session.

13. A user terminal according to Claim 12 further comprising

a key information generating means to which a public key of the user terminal is input and which generates a key information relating to the public key;

a session key generating means to which a private key of the user terminal and an public key of an application server are input and which calculates a session secret key which is shared with the application server;

and a packet cryptographic processing means to which a packet to be transmitted from the user terminal and the session secret key are input and which applies a processing to the transmitted packet which guarantees that there is no forgery in the packet by the session secret key;

the user authentication information transmitting means being means to which the key information is also input and which transmits the key information together with the user authentication information.

14. A user terminal according to Claim 12, further comprising

a key information generating means to which an authentication purpose shared secret key which is shared with the application server and a session dependent information which changes each time a session is established are input and which generates a key information by processing the session dependent information by the authentication purpose shared secret key;

the user authentication information transmitting means being means to which the key information is also input and which transmits the key information together with the user authentication information.

15. An application server in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication; comprising

a session establishing means for establishing a session with a user terminal;

a ticket memory means in which a ticket transmitted from the user terminal is stored;

an address comparison means to which a source address of a service request packet which is transmitted from the user terminal and received through the established session is input and which determines whether or not the source address coincides with an address contained in the ticket stored in the ticket memory means;

and a service providing means to which an output indicating a coincidence from the address comparison means is input and which transmits packets for providing a service to the user to the user terminal.

16. An application server according to Claim 15, further comprising

a ticket verifying means to which the ticket in the received packet is input and which verifies the authenticity of the ticket and prevents the ticket from being stored in response to a verification output which indicates the absence of the authenticity.

17. An application server according to Claim 16, further comprising

a session key generating means for calculating a session secret key which is shared with the user terminal from a private key of the application server and an public key of the user terminal;

and a packet verifying means for verifying whether or not a packet received from the user terminal is forged using the session secret key and for preventing the ticket from being stored in response to a verification output indicating the presence of a forgery.

18. An application server according to Claim 17 in which the ticket verifying means is means to which a packet which has been verified by the packet verifying means as not forged is input and which verifies whether or not the key information relating to the public key of the user terminal corresponds to the public key of the user terminal which has been used in the calculation of the session secret key.

19. An application server according to Claim 16 in which the ticket verifying means is means to which an authentication purpose shared secret key which is shared with the user terminal and a session dependent information which changes each time a session is established are input and which processes the session dependent information using the authentication purpose shared secret key, collates a result of the processing against the key information in the ticket and verifies the authenticity of the ticket by seeing whether or not a matching between the result of processing and the key information applies.

20. An application server according to one of Claims 16, 18 and 19 in which the ticket verifying means comprises means for verifying whether or not the source address of the received packet coincides with the address contained in the ticket within the packet and for preventing the ticket from being stored in response to a detection output which indicates a non-coincidence.

21. An authentication server program for allowing a computer to function as an authentication server as defined in one of Claims 7 to 11.

22. A user terminal program for allowing a computer to function as a user terminal according to one of Claims 12 to 14.

23. An application server program for allowing a computer to function as an application server according to one of Claims 15 to 20.